Executive Summary
KNOWiNK PollPad 3.0.1 Electronic Poll Book System

KNOWiNK applied for certification of the PollPad 3.0.1 electronic poll book system on January 3, 2022. Through the formal California contracting process and pursuant to California Elections Code section 19285, the Secretary of State awarded a contract to SLI Compliance (SLI) as the state-approved testing contractor in June of 2021. Testing concluded in early April 2022.

Electronic poll books replace the paper roster voter check-in model. Electronic poll books allow poll workers to process voters in approximately 35 to 40 seconds. They are also coupled with built-in election management and reporting tools designed to give election administrators real-time access to monitor their election. All electronic poll book devices deployed in the election connect to a central hub where voter check-in data is securely transferred in near real time. This tool allows election administrators to oversee the operation of individual voting locations and devices, including battery life of the device, average check-in times, or the number of ballots issued or spoiled.

The testing included: (1) Accessibility, Usability and Privacy Testing, (2) Software Testing, (3) Security and Telecommunications Testing, (4) Functional Testing, and (5) Volume Testing.

1. **Accessibility, Usability and Privacy Testing**

   Accessibility, usability (All Users Exp) and privacy testing, tests the system specialized focus on voters with accessibility needs. The goal is to test and confirm the system's ability to allow for voters with accessible needs to mark and cast their votes privately and independently. SLI evaluated the PollPad against the applicable portions of the Web Content Accessibility Guidelines (WCAG) 2.0 and Section 508 of the Rehabilitation Act of 1973 for compliance. One hundred and forty-three (143) requirements were reviewed and five (5) requirements were not met. All unmet requirements were associated to the same findings within the system. All findings were limited to non-voter facing functionality and would not prevent or hinder a voter with accessibility needs from independently participating in the check-in process at a polling location. However, KNOWiNK has committed to resolving these issues in the next version of the system.

   All five (5) of the following findings were related to the Bluetooth keyboard not having proper access to all fields on certain pages of the electronic poll book iPad application. When navigating through a page on the application utilizing a Bluetooth keyboard, a user utilizes the "Tab" key to move between fields. In some instances, the user would not be able to move past a particular field utilizing the "Tab" key as the courser will get stuck on a field.

   - **WCAG 2.0 § 2.1 - Make all functionality available from a keyboard.**
   - **WCAG 2.0 § 2.1.1 - All applicable page functionality is available using the keyboard.**
   - **WCAG 2.0 § 2.1.2 - Keyboard focus is never locked on one element. The user can navigate to and from all navigable page elements using only a keyboard.**
   - **WCAG 2.0 § 2.1.3 - All page functionality is available using the keyboard.**

- **Section 508 § 1194.21 - (l) When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.**

2. Software Testing (Source Code Review)

Software testing (also known as source code review) is a line-by-line review of all the computer code of the system for any errors, anomalies, or malicious code. The KNOWiNK PollPad 3.0.1 electronic poll book system had over 308,000 lines of computer code.

One (1) issue was identified within the PollPad source code. The following discrepancy pertains to KNOWiNK's ePulse web-based monitoring platform and is considered by SLI a non-functional issue of no impact to overall system security.

- **Lack of Header Comments, Multiple Instances**
  Header comments, regarding programming languages, are used to identify a file, what it contains, its purpose, and a small description of what the code is solving. For example, a module within the code that solves ballot layout logic (rotation, languages, character limitations). The actual outcome for this review was a determination that a large number of file/module header comments were insufficient or missing.

3. Security and Telecommunications Testing (Red Team)

Security and telecommunications testing is testing that examines the overall security and integrity of the system. SLI performed Security and Telecommunications testing on the PollPad. During testing, a full review of the PollPad system was performed to analyze for findings against applicable requirements. Five (5) issues were identified during testing. The following discrepancies pertain to KNOWiNK's ePulse web-based monitoring platform, which is considered the PollPad systems back-end. The discrepancies are considered by SLI to be of minimal impact to overall system security and successfully mitigated via KNOWiNK's implementation of Amazon Web Service Security Suite services, firewalls, network hardening techniques, input sanitization techniques, and virus scanning technologies.

- **One (1) Password Field with Autocomplete Enabled**
  - The ePulse web application has one field that is set to remember user credentials. The username and password entered by the user are stored on their local computer. The stored credentials can be captured by an attacker who gains control over the user's computer.

- **One (1) Instance of Cross-Site Scripting (DOM-Based)**
  - Cross-site Scripting allow attackers to input strings of executable malicious code into the web application. Malicious code is injected into the website's content, making it a part of the website, and thus allowing it to affect victims who may visit or view that website.

- **One (1) Instance of Strict Transport Security Not Enforced**
  - The ePulse web application fails to prevent users from connecting to it over unencrypted connections.

- **Multiple Instances of DOM-based Link Manipulation**
  - This allows attackers to control a target within the current page, such as a clickable link. For example, an attacker might be able to use this vulnerability to construct a link that, if visited by another user, can cause the user to submit sensitive data to a server controlled by the attacker.

- **One (1) Instance of Client-Side HTTP Parameter Pollution (Reflected)**
  - In one instance, the ePulse web application embeds user input in URLs in an unsafe manner. An attacker can use this vulnerability to construct a URL that, if visited by another application user, may result in unexpected side effects. For example, an attacker can create a vulnerable link with the application, after the user has clicked on it, the intended malicious behavior will be performed, affecting the user and the web application.

4. Functional Testing

Functional testing examines the system to the extent to which the system is accurate, efficient, reliable, and in compliance with the applicable regarding electronic poll book laws and standards. SLI configured the electronic poll books and exercised their functionality to provide verification of expected functions of the system as outlined in the vendor provided technical documentation, execution of test cases and verification of the electronic poll book's compliance with State statutes and regulations. During the examination, all electronic poll book functions outlined in the KNOWiNK PollPad 3.0.1 User Guide documentation were exercised.

During testing, two (2) issues related to minor documentation discrepancies were identified and provided to KNOWiNK for modification. The documentation was subsequently modified, and the changes verified by Secretary of State Staff.

There were no issues related to the hardware or software encountered during testing.

5. Volume Testing

The Volume Test simulates conditions in which the electronic poll book system would be used on Election Day. Ten (10) electronic poll book units were tested during the volume test. For approximately two days, over 1,500 mock voters were processed on the KNOWiNK Poll PadPollPad 3.0.1 electronic poll book system. Zero (0) unexpected results or issues were encountered during the Volume Test.

Conclusion

The KNOWiNK PollPad 3.0.1 electronic poll book system meets applicable California, HAVA, and Federal Elections laws. The system does however have some remaining findings, which KNOWiNK will address or has addressed in the appropriate mitigation areas of this report.

It is OVSTA's recommendation that the KNOWiNK PollPad 3.0.1 system be conditionally approved.